

REMARKS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-30 are pending. Claims 11, 20, 21, 23-26, and 30 have been amended by the present amendment. The changes to the claims are supported by the originally filed specification and do not add new matter.¹

In the outstanding Office Action, Claims 25 and 30 were rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the written description requirement; Claims 1-3, 5, 9-13, 15, 20, 21, 23, 24, and 26-30 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent Application Publication No. 2003/0101342 to Hansen; Claims 22, 25, and 30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hansen in view of U.S. Patent No. 7,130,069 to Honma; Claims 6-8 and 16-18 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hansen in view of U.S. Patent No. 6,785,812 to Botham, Jr. et al. (hereinafter “Botham”); and Claims 4, 14, and 19 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Hansen in view of U.S. Patent No. 6,233,618 to Shannon.

REJECTION UNDER 35 U.S.C. § 112

Applicants respectfully submit that the rejections of Claims 25 and 30 under 35 U.S.C. § 112, first paragraph, are rendered moot by the present amendments to those claims. In particular, Claims 25 and 30 have been amended to no longer recite “if the request for transmitting said stored document is determined to include the second password”. Accordingly, the rejections of Claims 25 and 30 under 35 U.S.C. § 112, first paragraph, are believed to have been overcome.

¹ See, e.g., Figs. 14-16 and the discussion related thereto in the originally filed specification.

REJECTION UNDER 35 U.S.C. § 102

Previously presented Claim 1 is directed to a file transfer system, comprising:

a file management server comprising a web page configured to manage a transfer of files and to allow the files to be accessed subject to a first password through the web page;

a file transmitting terminal configured to store a file and a second password for accessing the file, the second password being associated with the file;

a file receiving terminal; and

a mobile terminal,

wherein

said file management server, said file transmitting terminal, said file receiving terminal, and the mobile terminal are connected to each other via a network;

said file transmitting terminal is configured to transmit, to said file management server, the file and the second password as a part of an authentication condition for accessing the file, through the web page;

said file management server is configured to store and to correlatingly manage the file and the second password transmitted from said file transmitting terminal;

said mobile terminal is configured to transfer an address of a particular file receiving terminal that is permitted to access the file, to said file management server through the web page;

said file management server is configured to store and to correlatingly manage the address of said particular file receiving terminal with the file;

said file receiving terminal is configured to transmit to said file management server a request for transferring the file; and

in response to the request transmitted by said file receiving terminal, if an address of said file receiving terminal and the address of the particular file receiving terminal transferred by the mobile terminal are determined to match, and if the request transmitted by said file receiving terminal is determined to include the second password, said file management server is configured to transfer the file to said file receiving terminal.

Regarding the rejection of Claim 1 under 35 U.S.C. § 102(e), Hansen is directed to a computer-based secure printing system. In particular, Hansen discusses a printing system that includes a printer, a mobile computing device for holding a security key and instructions for printing the document and having a communication module for activating the printer to print the document when the mobile computing device is within a select proximity of the printer.²

However, it is respectfully submitted that Hansen fails to disclose said file management server is configured to store and to correlatingly manage the address of said particular file receiving terminal with the file. Rather, as cited in the Office Action, Hansen simply discusses a mobile computing device 16 and/or computer workstation 18 submits a request that a document be held at a server 40 for printing at a printing facility such as printing station 12.³ Hansen discusses the secure server 40 acts to hold documents in storage and communicates with one or more printing stations 12 to supply documents for printing upon request.⁴ Further, with respect to the cited identify printer function 128, Hansen discusses that the identify printer function 128 permits the user to identify a specific printer (e.g., printer 30 at printing station 12).⁵ Hansen does not disclose that the secure server 40 (i.e., the asserted file management server) is configured to *store and correlating manage* an identification of a specific printer (i.e., the asserted address of a particular file receiving terminal) *with a corresponding document* (i.e., the asserted file).

Further, it is respectfully submitted that Hansen fails to disclose in response to the request transmitted by said file receiving terminal, if an address of said file receiving terminal and the address of the particular file receiving terminal transferred by the mobile terminal are determined to match, and if the request transmitted by said file receiving terminal is

² See Hansen, Abstract.

³ Id. at paragraph [0027].

⁴ Id. at paragraph [0025].

⁵ Id. at paragraph [0031].

determined to include the second password, said file management server is configured to transfer the file to said file receiving terminal. Rather, with respect to the identification of a specific printer, Hansen discusses that a document is identified to a commercial printer 164 at a first point in time but not printed until a second point in time when the user is within a select proximity of printer 164 to insure its confidentiality. Further, Hansen discusses that alternatively, the user optionally chooses not to identify the document at all until the user is within a select proximity of commercial printer 164. In this case, Hansen discusses that the mobile computing device 158 does not identify and post the document to the commercial server 160 until mobile computing device 158 is within the select proximity of the commercial printer 164.⁶ Hansen does not disclose that *in response to a request transmitted from a printer* (i.e., the asserted file receiving terminal) the secure server 40 (i.e., the asserted file management server) is configured to transfer a document (i.e., the asserted file) to the printer, if the identification of the specific printer (i.e., the asserted address of said particular file receiving terminal) and the address of the printer *are determined to match*.

Amended Claim 11 recites, *inter alia*,

a second storage unit configured to store and to correlatingly manage an address of a particular file receiving terminal that is to be allowed to access the file with the file, the address being transmitted from the mobile terminal through the web page; and

a file transferring unit configured to, in response to a request for transferring said file stored in said first storage unit from said file receiving terminal, transfer said file to said file receiving terminal if an address of said file receiving terminal and the address of the particular file receiving terminal transmitted from the mobile terminal are determined to match, and if the request for transferring said file is determined to include the second password.

Amended Claim 20 recites, *inter alia*,

⁶ See Hansen, paragraphs [0035] and [0036].

storing and correlatingly managing, by the information processing apparatus, an address of a particular file receiving terminal that is allowed to access the file with the file, the address being transmitted from a mobile terminal through the web page;

...; and

in response to the request, transmitting, by the information processing apparatus, said file to said file receiving terminal if an address of said file receiving terminal and the address of the particular file receiving terminal transmitted from the mobile terminal are determined to match, and if the request for transmitting said file is determined to include the second password.

Amended Claim 21 recites, *inter alia*,

storing and correlatingly managing an address of a particular file receiving terminal that is to be allowed to access the file with the file, the address being transmitted from a mobile terminal through the web page;

...; and

in response to the request, transmitting said file to said file receiving terminal if an address of said file receiving terminal and the address of the particular file receiving terminal transmitted from the mobile terminal are determined to match, and if the request for transmitting said file is determined to include the second password.

Previously presented Claim 22 recites, *inter alia*,

said stored document management server is configured to store and to correlatingly manage the address of said particular image forming apparatus with the stored document;

...; and

in response to the request transmitted by the second image forming apparatus, if an address of said second image forming apparatus and the address of the particular image forming apparatus transferred by the mobile terminal are determined to match, and if the request for transferring the stored document is determined to include the second password, said stored document management server is configured to transfer the stored document to said second image forming apparatus.

Amended Claim 23 recites, *inter alia*,

a second storage unit configured to store and to correlatingly manage an address of a particular image forming apparatus that is to be allowed to access the stored document with the stored document, the address being transmitted from the mobile terminal through the web page; and

a stored document transferring unit configured to, in response to a request for transferring said stored document stored in said first storage unit from said second image forming apparatus, transfer said stored document to said second image forming apparatus if an address of said second image forming apparatus and the address of the particular image.

Amended Claim 24 recites, *inter alia*,

a first image forming apparatus configured to manage a transfer of stored documents and to allow the stored documents to be accessed subject to a first password, to store a stored document and a second password for accessing the stored document, and to store and to correlatingly manage an address of a particular image forming apparatus that is permitted to access the stored document with the stored document, the second password being associated with the stored document.

Amended Claim 25 recites, *inter alia*,

said stored document management server is configured to store said stored document and said second password, and to store and to correlatingly manage an address of a particular image forming apparatus that is permitted to access the stored document with the stored document.

Amended Claim 26 recites, *inter alia*,

a communication unit configured to exchange data via said network, and, subject to a first password, to receive a stored document and a second password from said other image forming apparatus, the second password being associated with the stored document and the other image forming apparatus being configured to store and correlatingly manage an address of a particular image forming apparatus that is permitted to access the stored document with the stored document.

Amended Claim 30 recites, *inter alia*,

said communication unit is configured to, in response to reception of a request for transmitting said stored document from said user terminal, transmit said stored document and said second password to said stored document management server, the stored document management server being configured to store and correlatingly manage an address of a particular file

receiving terminal that is permitted to access the stored document with the stored document.

As noted above, Hansen fails to disclose the file management server of Claim 1. Thus, Hansen fails to disclose the storage unit and file transferring unit of Claim 11, the storing and correlatingly managing step and transmitting step of Claims 20 and 21, the stored document management server of Claims 22 and 25, the second storage unit and stored document transferring unit of Claim 23, the first image forming apparatus of Claim 24, and the communication unit of Claims 26 and 30. Accordingly, it is respectfully submitted that Claims 11, 20-26, and 30 (and all associated dependent claims) patentably defines over Hansen.

REJECTION UNDER 35 U.S.C. § 103

Regarding the rejections of dependent Claims 22, 25, and 30 under 35 U.S.C. § 103(a), it is respectfully submitted that Honma fails to remedy the deficiencies of Hansen, as discussed above. Accordingly, it is respectfully submitted that dependent Claims 22, 25, and 30 patentably define over any proper combination of Hansen and Honma.

Regarding the rejections of dependent Claims 6-8 and 16-18 under 35 U.S.C. § 103(a), it is respectfully submitted that Botham fails to remedy the deficiencies of Hansen, as discussed above. Accordingly, it is respectfully submitted that dependent Claims 6-8 and 16-18 patentably define over any proper combination of Hansen and Botham.

Regarding the rejections of dependent Claims 4, 14, and 19 under 35 U.S.C. § 103(a), it is respectfully submitted that Shannon fails to remedy the deficiencies of Hansen, as discussed above. Accordingly, it is respectfully submitted that dependent Claims 4, 14, and 19 patentably define over any proper combination of Hansen and Shannon.

CONCLUSION

Thus, it is respectfully submitted that independent Claims 1, 11, 20-26, and 30 (and all associated dependent claims) patentably define over Hansen, Honma, Botham, and Shannon.

Consequently, in view of the present amendment and in light of the above discussion, the outstanding grounds for rejection are believed to have been overcome. The application as amended herewith is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.


Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Customer Number

22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 03/06)



James J. Kulbaski
Attorney of Record
Registration No. 34,648

Johnny Ma
Registration No. 59,976

3387942_1.DOC